JAP:DCP

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

- - - - - - - - - - - - - - - - - -X

IN THE MATTER OF AN APPLICATION OF THE UNITED STATES OF AMERICA FOR ORDERS AUTHORIZING THE DISCLOSURE OF LOCATION DATA RELATING TO A SPECIFIED WIRELESS MOBILE DEVICE

- - - - - - - - - - - - - - - - - -X

13 MISC 201

FILED UNDER SEAL

AFFIDAVIT IN SUPPORT OF APPLICATION
(Fed. R. Crim. P. 41; T. 18, U.S.C., §§ 2703(c)(1)(A), 3103a and 3117; T.28, U.S.C., § 1651(a))

EASTERN DISTRICT OF NEW YORK, SS:

I, THOMAS THOMPSON, being first duly sworn, hereby depose and state as follows:

1. I make this affidavit in support of an application for a search warrant under Federal Rule of Criminal Procedure 41 and 18 U.S.C. § 2703(c)(1)(A) for information about the location of the cellular mobile device assigned MAC address 001D880A2262, subscribed to by Rosilesisi Ceballo, 459 Central Avenue, Brooklyn, New York 11221 (the "SUBJECT MOBILE DEVICE"), whose wireless mobile device service provider is Clearwire Corporation (the "Service Provider"). The SUBJECT MOBILE DEVICE is described herein and in Attachment A, and the location information to be seized is described herein and Attachment B.

2. I have been a Special Agent of the FBI since December 2004, and am currently assigned to the New York Office. Since September 2007, I have been assigned to a Crimes Against Children squad. I have been assigned to investigate violations of criminal law relating to the sexual exploitation of children. I have gained expertise in this area through training in classes and daily work related to conducting these types of investigations. As part of my responsibilities, I have been involved in the investigation of numerous child pornography cases and have reviewed thousands of photographs depicting children (less than eighteen years of age) being sexually exploited by adults. Through my experience in these investigations, I have become familiar with methods of determining whether a child is a minor. I am also a member of the Eastern District of New York Project Safe Childhood Task Force.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. Because the purpose of this affidavit is limited to demonstrating probable cause for the requested warrant, it does not set forth all of my knowledge about this matter. In addition, when I rely on statements made by others, such statements are set forth only in part and in substance unless otherwise indicated.

4. Based on the facts set forth in this affidavit, there

is probable cause to believe that the distribution of child pornography, in violation of 18 U.S.C. § 2252(a)(2), has been committed, and is being committed, by the user of the SUBJECT MOBILE DEVICE ("the TARGET"). There is also probable cause to believe that the TARGET has used, and is currently using, the SUBJECT MOBILE DEVICE to distribute child pornography. There is therefore probable cause to believe that the location information, including but not limited to E-911 Phase II data (or other precise location information) concerning the SUBJECT MOBILE DEVICE (the "REQUESTED INFORMATION"),[1] as described in Attachment B, will constitute evidence of these criminal violations, and will lead to the identification of individuals who are engaged in the commission of these offenses, as well as victims of these offenses.

[1] Such information shall, where other information is unavailable, include records reflecting the tower and antenna face ("cell site") used by the SUBJECT MOBILE DEVICE at the start and end of online connection. In requesting cell site information, the government does not concede that such cell site records — routinely retained by wireless carriers as business records — may only be obtained via a warrant issued on probable cause. See In re Application, 632 F. Supp. 2d 202 (E.D.N.Y. 2008) (authorizing prospective acquisition of cell-site records under combined authority of 18 U.S.C. 2703(d) & 3121 et seq.); In re Application, 460 F. Supp. 2d 448 (S.D.N.Y. 2006) (same).

PEER-TO-PEER FILE SHARING

5. Peer-to-peer file-sharing ("P2P") is a method of communication available to Internet users through the use of special software. Computers linked together through the Internet using this software form a network that allows for the sharing of digital files between users on that network. A user first obtains the P2P software, which can be downloaded from the Internet. In general, P2P software allows the user to set up files on a computer to be shared with others running compatible P2P software. A user obtains files by opening the P2P software on the user's computer, and conducting searches for files that are currently being shared on another user's computer.

6. The latest evolution of P2P software is a program that allows a user to set up his own private P2P network of contacts. File-sharing through this new and publicly available P2P file-sharing program is limited only to other users who have been added to a private list of "friends." A new user is added to a list of friends by request. Acceptance of a friend request will allow that new user to download files from the user who sent the friend request. The new user can then browse the list of files that the other user has made available to download, select desired files from this list, and download the selected files. The downloading of a

file occurs through a direct connection between the computer requesting the file and the computer containing the file.

7. One aspect of P2P file sharing is that multiple files may be downloaded in parallel, which permits downloading more than one file at a time.

8. A P2P file transfer is assisted by reference to an Internet Protocol (IP) address. This address, expressed as four sets of numbers separated by decimal points, is unique to a particular computer during an online session. The IP address provides a unique location making it possible for data to be transferred between computers.

9. Third-party software ("Network Monitoring Program") is available to identify the IP address of the P2P computer sending the file. Such software monitors and logs Internet and local network traffic.

PROBABLE CAUSE

10. On January 4, 2013, FBI New Haven notified a FBI New York Special Agent working in an online undercover capacity ("Undercover Agent") that the online user Ovidquintana was currently signed on to a peer-to-peer (P2P) program, which is publicly-available, and he was sharing child pornography. FBI New Haven provided SA Thompson the password, "123456", to Ovidquintana's password protected folders. FBI New Haven had obtained the password

through a consensual takeover account ("UC ACCOUNT #1"). The Undercover Agent then signed on to the P2P file sharing program as UC ACCOUNT #2 via an Internet connected computer located at the FBI New York Office. The Undercover Agent memorialized the session by intermittent video capture using a publicly available computer program. Any download activity from the session was monitored via a Network Monitoring Program.

11. The Undercover Agent previously sent an invite to Ovidquintana that was accepted by Ovidquintana on December 7, 2012. Upon signing on to P2P program as UC ACCOUNT #2, the Undercover Agent observed that the user Ovidquintana was online. Ovidquintana was sharing nine password protected folders. Ovidquintana communicated in a private message with the Undercover Agent that his password was "123456" (same password provided by FBI New Haven). The Undercover Agent entered the password and browsed through Ovidquintana's shared files and numerous files had filenames and thumbnails indicative of child pornography.

12. The Undercover Agent downloaded one (1) image[2] file

[2] Although still images of apparent child pornography can be created using "morphing" technology and the identity of these minors are not known to law enforcement (i.e., the identity and age of the children have not been discovered by law enforcement), it appears that these images involve the use of actual (i.e. non-virtual) minors engaging in sexually explicit conduct. This conclusion is also based upon my consultation with other agents experienced in determining whether child pornography images depict real children. In addition,

from Ovidquintana and the Affiant has reviewed the file. The file, which is available for the Court's review, is described as follows:

a. !!!**new _baby_fuck(2).jpg** is an image of a partially clothed female infant, less than one years old, lying down and an adult male's penis is touching the girls's vagina.

13. Ovidquintana then deleted UC ACCOUNT #2 from his buddy list. On February 8, 2013, the Undercover Agent signed on to the P2P program as UC ACCOUNT #3 and observed that Ovidquintana had accepted the invite from UC ACCOUNT #3 and Ovidquintana was currently online. Ovidquintana was sharing 10 password protected folders. The Undercover Agent entered the password, "123456"; the same password Ovidquintana provided to UC ACCOUNT #1 and UC ACCOUNT #2. The Undercover Agent communicated to Ovidquintana in a private message that he had Ovidquintana's password to the protected folders. The Undercover Agent browsed through Ovidquintana's shared files and numerous files had filenames and thumbnails indicative of child pornography (CP); including infants and toddlers.

14. On February 15, 2013, the Undercover Agent signed on

---

based upon my experience in child pornography investigations, I have found that collectors of child pornography generally have in their collections both images which depict children known to law enforcement and images in which the identities of the children depicted are not yet known to law enforcement. Moreover, where, as here, an individual is a member of a hardcore pedophile/child pornography network which is not accessible by casual web-browsing, the likelihood that such an individual is in possession of child pornography depicting real children is extremely high.

to the P2P program as UC ACCOUNT #3 and observed that Ovidquintana was online. The Undercover Agent downloaded four (4) image files depicting child pornography from Ovidquintana and the Affiant has reviewed the files. All of the files are available for the Court's review; two of the files are described as follow:

a. ! **Cum0004.jpg** is an image of a nude prepubescent female, approximately five years old, lying down with her vagina exposed. An adult male's penis is touching the girl's vagina. A white substance, that appears to be semen, is on the penis and on the girl.

b. !!!!!**BABYboy_dad44789.jpg.jpg** is an image of a nude infant boy, approximately one year old, and a nude adult male in a bathtub. The adult male's penis appears to be in the mouth of the infant boy.

15. The Undercover Agent used the Network Monitoring Program to identify the IP addresses, utilized by Ovidquintana, on all three dates as 50.14.136.181, 50.14.231.9, and 96.25.225.60. Open source database searches revealed all the IP addresses were registered to Clearwire Corporation.

16. Administrative subpoenas were served on Clearwire Corporation for the three IP addresses. Clearwire could only provide subscriber information for the two most recent undercover dates, February 8, 2013, and February 15, 2013. The subscriber associated with these IP addresses was "Rosilesisi Ceballo", customer ID "3038835", billing address "459 Central Ave, Brooklyn,

NY 11221." The subscriber is using a USB mobile broadband device, SUBJECT MOBILE DEVICE, that gets plugged into a laptop or desktop computer[3] and the device's MAC address is "001D880A2262." Open source database searches revealed that Rosilesisi Ceballo recently associated with the above Brooklyn, NY, residence and a residence in Queens, NY.

17. There is therefore probable cause to believe that the REQUESTED INFORMATION will lead to evidence regarding the activities described above. The REQUESTED INFORMATION is necessary to assist law enforcement agents in conducting surveillance; determine the location of child pornography; and assist law enforcement officers in obtaining a search warrant at the location where the child pornography is being stored.

AUTHORIZATION REQUEST

18. WHEREFORE, pursuant to Federal Rule of Criminal Procedure 41 and 18 U.S.C. § 2703(c)(1)(A), it is requested that the Court issue a warrant and Order authorizing agents to obtain the REQUESTED INFORMATION for a period of 30 days.

[3] A USB Mobile Device is functionally similar to a cellular telephone in that it permits a user to access the internet using a cellular signal. Unlike a cellular telephone, a USB Mobile Device cannot be used to make incoming or outgoing telephone calls.

19. IT IS FURTHER REQUESTED that the Court direct the Service Provider to assist law enforcement by providing all information, facilities and technical assistance needed to ascertain the REQUESTED INFORMATION, and further direct the service provider to initiate a signal to determine the location of the SUBJECT MOBILE DEVICE on the service provider's network or with such other reference points as may be reasonably available and at such intervals and times as directed by the law enforcement officer serving the proposed order, and to furnish the technical assistance necessary to accomplish the acquisition unobtrusively and with a minimum of interference with such services as that provider accords the user(s) of the SUBJECT MOBILE DEVICE, for a period of 30 days. Reasonable expenses incurred pursuant to this activity will be processed for payment by the Federal Bureau of Investigation.

20. IT IS FURTHER REQUESTED that the Court authorize execution of the warrant at any time of day or night, owing to the potential need to locate the SUBJECT MOBILE DEVICE outside of daytime hours.

21. IT IS FURTHER REQUESTED, pursuant to 18 U.S.C. § 3103a(b) and Federal Rule of Criminal Procedure 41(f)(3), that the Court authorize the officer executing the warrant to delay notice until 30 days after the collection authorized by the warrant has been completed or any extension thereof. This delay is justified because

there is reasonable cause to believe that providing immediate notification of the warrant may have an adverse result, as defined in 18 U.S.C. § 2705. Providing immediate notice to the subscribers or users of the SUBJECT MOBILE DEVICE would seriously jeopardize the ongoing investigation, as such disclosure would give the targets of the investigation an opportunity to destroy evidence, harm or threaten victims or other witnesses, change patterns of behavior, and flee from and evade prosecution. Moreover, to the extent that the warrant authorizes the seizure of any wire or electronic communication (as defined in 18 U.S.C. § 2510), or any stored wire or electronic information, there is reasonable necessity for the seizure for the reasons set forth above.

10. IT IS FURTHER REQUESTED that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing these documents is necessary because the items and information to be seized are relevant to an ongoing investigation into the criminal organizations, and not all of the targets of this investigation will be searched at this time. Based upon my training and experience, I have learned that criminals actively search for criminal affidavits and search warrants via the internet, and disseminate them to other criminals as they deem appropriate, e.g., by posting them publicly through online forums.

Therefore, premature disclosure of the contents of this affidavit and related documents will seriously jeopardize the investigation, including by giving targets an opportunity to flee or continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, and notify confederates.

11. IT IS FURTHER REQUESTED that, pursuant to 18 U.S.C. § 2705(b) and for the reasons stated above, it is further requested that the Court issue an Order commanding Clearwire Corporation not to notify any person (including the subscribers or customers of the account listed in the attached warrant) of the existence of the attached warrant until further order of the Court.

Dated: Brooklyn, New York
March 11, 2013

Thomas Thompson
Special Agent
Federal Bureau of Investigation

Sworn to before me the 11th day of March, 2013

s/Lois Bloom

THE HONORABLE LOIS BLOOM
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK

ATTACHMENT A

Property To Be Searched

1. The cellular mobile device assigned the MAC address 001D880A2262, with customer ID 3038835 (the "SUBJECT MOBILE DEVICE"), whose wireless service provider is Clearwire Corporation, a company headquartered at 1250 I Street NW, Suite 901, Washington DC 20005.

2. Information about the location of the SUBJECT MOBILE DEVICE that is within the possession, custody, or control of Clearwire Corporation.

ATTACHMENT B

Particular Things to be Seized

All information about the location of the SUBJECT MOBILE DEVICE described in Attachment A for a period of thirty days, during all times of day and night. "Information about the location of the SUBJECT MOBILE DEVICE " includes all available E-911 Phase II data, GPS data, latitude-longitude data, and other precise location information, as well as all data about which "cell towers" (i.e., antenna towers covering specific geographic areas) and "sectors" (i.e., faces of the towers) received a radio signal from the cellular mobile device described in Attachment A.

To the extent that the information described in the previous paragraph (hereinafter, "Location Information") is within the possession, custody, or control of Clearwire Corporation, Clearwire Corporation is required to disclose the Location Information to the government. In addition, Clearwire Corporation must furnish the government all information, facilities, and technical assistance necessary to accomplish the collection of the Location Information unobtrusively and with a minimum of interference with Clearwire Corporation's services, including by initiating a signal to determine the location of the SUBJECT MOBILE DEVICE on Clearwire Corporation's network or with such other reference points as may be reasonably available, and at such intervals and times directed by the government. The government shall compensate Clearwire Corporation for reasonable expenses incurred in furnishing such facilities or assistance.

To the extent that the Location Information includes tangible property, wire or electronic communications (as defined in 18 U.S.C. § 2510), or stored wire or electronic information, there is reasonable necessity for the seizure. See 18 U.S.C. § 3103a(b)(2).

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

- - - - - - - - - - - - - - - - - x

IN RE APPLICATION OF THE UNITED STATES OF AMERICA FOR AUTHORIZATION TO OBTAIN LOCATION DATA CONCERNING A MOBILE DEVICE ASSIGNED MAC ADDRESS 001D880A2262

- - - - - - - - - - - - - - - - - x

TO BE FILED UNDER SEAL

ORDER

13 MISC 201

Application having been made for a search warrant under Federal Rule of Criminal Procedure 41 and 18 U.S.C. §§ 2703(c)(1)(A) for information about the location of the cellular mobile device assigned MAC address 001D880A2262, subscribed to by Rosilesisi Ceballo, 459 Central Avenue, Brooklyn, New York 11221 (the "SUBJECT MOBILE DEVICE"), whose wireless mobile device service provider is Clearwire Corporation (the "Service Provider"), as further described in Attachment B to the search warrant (the "REQUESTED INFORMATION");

The Court finds that there is probable cause to believe that the REQUESTED INFORMATION will constitute or lead to evidence of violations of 18 U.S.C. §§ 2252 and 18 U.S.C. §§ 2252A as well as to the identification of individuals who are engaged in the commission of these offenses. The Court also finds that there is reasonable cause to believe that providing immediate notification of the execution of the warrant may seriously jeopardize an ongoing investigation, including by giving targets an opportunity to flee

or continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, or notify confederates. See 18 U.S.C. §§ 2705(b)(2), 2705(b)(3) and 2705(b)(5). Furthermore, the execution of this warrant will not result in the seizure of any tangible property or any wire or electronic communication (as defined in 18 U.S.C. § 2510). To the extent that the warrant authorizes the seizure of any stored wire or electronic information, that seizure is expressly authorized by 18 U.S.C. § 2703(c)(1)(A).

IT IS HEREBY ORDERED pursuant to Federal Rule of Criminal Procedure 41 and 18 U.S.C. § 2703(c)(1)(A) that law enforcement officers, beginning at any time within ten days of the date of this Order and for a period not to exceed 30 days, may obtain the REQUESTED INFORMATION concerning the SUBJECT MOBILE DEVICE, with said authority to extend to any time of the day or night as required, including when the SUBJECT MOBILE DEVICE leaves the Eastern District of New York; all of said authority being expressly limited to ascertaining the physical location of the SUBJECT MOBILE DEVICE and expressly excluding the contents of any communications conducted by the user(s) of the SUBJECT MOBILE DEVICE.

It is further ORDERED that Clearwire Corporation (the "service provider") assist law enforcement by providing all information, facilities and technical assistance needed to ascertain the REQUESTED INFORMATION, including by initiating a signal to

determine the location of the SUBJECT MOBILE DEVICE on the service provider's network or with such other reference points as may be reasonably available and at such intervals and times as directed by the law enforcement agent serving the proposed order, and furnish the technical assistance necessary to accomplish the acquisition unobtrusively and with a minimum of interference with such services as the service provider accords the user(s) of the SUBJECT MOBILE DEVICE.

It is further ORDERED that the Federal Bureau of Investigation compensate the service provider for reasonable expenses incurred in complying with any such request.

It is further ORDERED that the Court's Order and the accompanying Affidavit submitted in support thereof be sealed until further Order of the Court, except that copies of the Court's Order in full or redacted form may be maintained by the United States Attorney's Office, and may be served on law enforcement officers, and other government and contract personnel acting under the supervision of such law enforcement officers, and the service provider as necessary to effectuate the Court's Order.

It is further ORDERED that this warrant be returned to the issuing judicial officer within 14 days after the termination of the monitoring period authorized by the warrant.

It is further ORDERED that, pursuant to 18 U.S.C. § 3103a(b) and Federal Rule of Criminal Procedure 41(f)(3), service of notice may be delayed for a period of 30 days after the termination of the monitoring period authorized by the warrant or any extension thereof.

It is further ORDERED under 18 U.S.C. § 2705(b) that Clearwire Corporation shall not disclose the existence of the attached warrant, or this Order of the Court, to the listed subscriber or to any other person, unless and until otherwise authorized to do so by the Court, except that Clearwire Corporation may disclose the attached warrant to an attorney for Clearwire Corporation for the purpose of receiving legal advice.

It is further ORDERED that this Order apply to any changed mobile telephone number subsequently assigned to the SUBJECT MOBILE DEVICE within the period of this Order.

It is further ORDERED that the application and this Order are sealed until otherwise ordered by the Court.

Dated: Brooklyn, New York
March 11, 2013

s/Lois Bloom

THE HONORABLE LOIS BLOOM
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK